STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

# INFORMATION INFRASTRUCTURE DEVELOPMENT RECOMMENDATIONS THROUGH ANALYSIS OF CURRENT INFORMATION TECHNOLOGY INFRASTRUCTURE, PLANS AND POLICIES

BY

COMMANDER JEFFREY L. ELLWOOD
United States Navy

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1998

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

# Information Infrastructure Development Recommendations through Analysis of Current Information Technology Infrastructure, Plans and Policies

by

Jeffrey L. Ellwood

Michael J. Morin
Professor of Doctrine
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

## ABSTRACT

AUTHOR: Jeffrey L. Ellwood

TITLE: Information Infrastructure Development Recommendations Through Analysis of Current Information Technology Infrastructure, Plans and Policies.

FORMAT: Strategy Research Project

DATE: 06 April 1998 PAGES: 30 CLASSIFICATION: Unclassified

The purpose of this paper is to analyze current Global, National, and Department of Defense policies and initiatives for information technology management and infrastructure, and to recommend courses of action for the development of these information infrastructures in support of the National Security Strategy and the National Military Strategy. This will be accomplished through a brief introduction into the information age and the information society, and the military influence on information and communication technologies development; a review of the policy, objectives, concepts and methods, and the resources outlined in the Information Technology Management (ITM) Strategic Plan, the Defense Information Infrastructure (DII) Master Plan, and the Global and National Information Infrastructure (GII, NII) initiatives.

## TABLE OF CONTENTS

# INTRODUCTION TO THE INFORMATION AGE AND THE INFORMATION SOCIETY

We are an Information society in a evolutionary status, and there are several common policies and initiatives in the Global, National, and Defense Information Infrastructure (GII, NII, DII) that are poised to launch us into an information revolution. Indeed, some think we have already reached the revolutionary stage. However, there are many areas which require further development and refinement to fully realize the status of an information revolution. To fully realize the potential of existing and emerging information and communications technologies we will examine the establishment and integration of this "information environment" on a national and global scale.

"What makes the information explosion so revolutionary is not that technology is advancing but the pace at which it improves. ... never before have societies been forced to adapt to a technology which for decades has been improving by an order of magnitude every three or four years. ...the rate at which information can be transmitted over long distances --looks set to continue at the rate of tenfold every three to four years, which translates into up to 1,000-fold per decade.[1]"

The present evolution of information and communications technologies break down into three modern phases[2]. The first phase, the development of the telephone, radio, and telegraph gave us first truly global communications. The military used the telegraph in the Civil War for logistics and intelligence. Telegraph and telephone linked capitols around the world, forever changing world politics. Radio enhanced communications at sea, led to the development of RADAR, was extensively used in WW1 for command, control, and communications, and in WW2 was used to spread German nationalism and propaganda.

The second phase, the television, computer, and the early satellites changed America after WW II from an industrial based economy to a service economy. Television, a qualitative improvement over radio, provided greater bandwidth and more powerful medium. It expanded the US culture globally, affected public opinion, and expanded the economy. Some say that westernization, consumerism and pro-democracy, spread into eastern Europe and sped the collapse of communism.

The military played significant roles in developing both computers and satellites. Computers provided a greater capacity to collect, analyze and utilize information. The early development of the computer was provided for by military need. Although the computer was developed at the University of Iowa in 1939, the British built the

"Colossus" computer to break the Nazi war codes. Satellites extended the global communications infrastructure and provided the capability for real-time global communications. The military launched its first communications satellite one year after Sputnik, in 1958. The first civilian communication satellite "Syncom III" was launched in 1964. A year later "Early Bird" was launched, with 240 voice or one television channel. Eventually INTELSAT was created, a global organization to create a global commercial system. INTELSAT brought us live coverage of the Apollo 11 moon landing.

The "impact" of this second modern revolution is complex, but most arguably affected the multinational corporation. It led to a global product division infrastructure, accelerated regionalization and globalization of business, and transformed international finance and banking. We'll discuss this in more depth later.

The third evolutionary phase is advanced information and communication technologies, which had six major technological impacts; increased speed, greater capacity, enhanced flexibility, greater access, more types of messages, and heightened demand.

The more important of these advanced technologies[3] are:

- Advanced semiconductors - in 1978 had 10K bits of data flow, in 1993 had 10 million bits of flow, a quadrupling every three years.

- Advanced computers - todays desktops are approaching the power of the CRAY computer of the 80's, and the next generation based on artificial intelligence is on the horizon.

- Fiber Optics - carry over a billion bits per second, over coppers 64K.

- Cellular technology - is replacing land line infrastructure expansion in developing countries such as India and some of the Caribbean countries.

- Satellite technology - has built an international communication infrastructure accessible by government, business, academia, and private organizations. It has made phone communication, electronic mail, teleconferencing and television both global and instantaneous.

- Advanced networking - the Internet - the government is working on the High Performance Computing and Communications program, linking different services and electronic mediums into one communication pathway and network.

- Improved human-computer interaction - Windows has made working with computers less fearful to people. Voice interaction and handwriting recognition are in their infancy, but promise to open computers to those still fearful of man-machine interaction.

- and finally, digital compression and transmission - digital is the language of computers, it is replacing analog phone, television wave, and data. Digital compression of data dramatically reduces files by identifying what is new information and what is old, sending only the new, resulting in a transmission length of 20 - 25% of an uncompressed message.

When looking at these technological advances in information and communications, we must ask; information quality vs. quantity, has it changed society sufficiently to warrant an information age or an information revolution? Information by itself means nothing, it is just data, it can be stored and transmitted, but until we use it and it becomes knowledge, wisdom, or experience, it does not have a profound effect on society. But at the rate at which it is advancing, it is poised to change society, to change the way we interact.

Electronic communication has changed many aspects of human interaction. It has changed the workplace, doing business at home is commonplace. We can do our shopping, buy plane tickets, make appointments, and communicate via E-mail. The Electronic Commerce Revolution is changing business from an inventory based system to an information based system. Commercenet provides detailed product information and on-line distribution systems to business. The Industrynet provides provides information and shopping for industrial products and services.

The structure of the commercial distribution system is changing. TV shopping networks and CD ROM catalogs are expanding. Associations, Realtors, and homebuilders are using this media. Resellers now process, pack, and ship products from manufacturers. Manufacturers and technology companies themselves now promote and sell direct. One could easily make a case that business has taken a lead in national and global information infrastructure development, and should lead the way.

To sustain this lead, business to business market and transaction processes need to move step by step to meet requirements, resolve the conflicts, and establish a common system for the consumer. And where are they doing this is the Internet. The Internet prototypes a global infrastructure. It holds the possibility of further transforming business commerce through electronic transaction, resolving some security concerns, and payment and settlement architectures in commerce and in business. This will require business and industry not only to recognize and utilize this media, but to develop new interfaces and marketing strategies.

Business is not the only ones affected by this evolution. The Internet and "civic networks" are extending the reach of democracy, deepening people's understanding of government and military issues, broadening participation, enabling more effective individual and group advocacy, and increasing civic interest.

International order will be affected by the expansion of the information environment. The nation-state will have to change, as happened to the Soviet Union, from a centralized government which controlled information and the economy. The Soviet Union was unable to keep up with global economics, lacking the connectivity and internal infrastructure to keep up with the world. This undoubtedly contributed to their collapse.

China and many other globally emerging countries and markets are still fighting these technologies, limiting connectivity to the Internet and the global infrastructure. They will have to change if they truly desire to emerge on the world market.

## ANALYSIS OF THE INFORMATION TECHNOLOGY MANAGEMENT STRATEGIC PLAN, THE DEFENSE INFORMATION INFRASTRUCTURE MASTER PLAN, AND THE DEFENSE, NATIONAL, AND GLOBAL INFORMATION INFRASTRUCTURE INITIATIVES.

The Global, National, and Defense Information Infrastructures (GII, NII, DII) plans and policies have several common goals.

The mission statement of the Global Information Infrastructure (GII) Commission[4] outlines several objectives and initiatives:

* Strengthen the leadership role of the private sector in the development of a diverse, affordable and accessible information infrastructure;

* Promote involvement of developing countries in the building and utilization of truly global and open information;

* Facilitate activities and identify policy options which foster effective applications of telecommunications, broadcasting and information technologies and services.

The key National Information Infrastructure (NII)[5] focuses are:

* Interoperability enables the diverse components of the information infrastructure -- networks, applications, devices, and systems -- to communicate smoothly and easily with each other. The key to interoperability is open interfaces, and reliance on the marketplace and the private sector-led voluntary standards process is the best way to develop open interfaces.

* Access to the NII must be widespread; that the marketplace will drive the availability of the networks, appliances, and services the people will need to use the NII; and as new NII services become widely adopted, policy makers should consider whether the marketplace has

achieved the goal of enabling all users to obtain essential NII services.

The Defense Information Infrastructure (DII) outlines the following vision and goals through the Information Technology Management (ITM) Strategic Plan[6]. The Information Technology Management (ITM) Strategic Plan was published by the Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence (ASDC3I) in March 1997 to provide overall direction and guidance for managing the Department's information resources. The ITM strategic Plan does not address specific programs or budgets, but serves as a framework for more specific DoD programs and initiatives.

The Vision Statement of the ITM Strategic Plan is: "Information superiority achieved through global, affordable and timely access to reliable and secure information for worldwide decision-making and operations.[7]" To realize this vision, four goals have been established:

GOAL 1 - "Become a mission partner".

GOAL 2 - "Provide services that satisfy customer information needs".

GOAL 3 - "Reform IT management processes to increase efficiency and mission contribution".

GOAL 4 - "Ensure DoD's vital information resources are secure and protected".

Let's expand these goals:

* "Become a mission partner" - to focus on mission support.

* "Provide services that satisfy customer needs" - to focus the information infrastructure on customer, information, service, and performance.

* "...Reform IT management..." - to highlight initiatives to streamline DoD policies and procedures.

* "Provide information assurance..." - to expedite implementation of information security practices and capabilities.

The architecture to support the goals of the ITM Strategic Plan is the Defense Information Infrastructure (DII). By definition, the DII is a web of communications networks, computers, software, databases, applications, weapons systems interfaces, data, security services, and other services that meet the information processing and transport needs of DoD users[8]. Not designed as a single program, the DII is a capability resulting from the integration of individual information management programs within the DoD.

The Defense Information Infrastructure (DII) Master Plan, (Version 6.0, June 27, 1997, updated October 23,1997), is a document for managing the DII evolution. It is a high level overview, descriptive in nature, reflecting DII policy, guidance, strategies, initiatives, and issues. The DII includes the information infrastructure of the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Defense Agencies, and the Combatant Commands. The scope of the infrastructure is not limited to the DoD and it interfaces with industry, government, academia, our allies, and other nations.

To support the information security aspects of the National Military Strategy and National Security Strategy we need to analyze the policy objectives, the concepts and methods, and the resources available as prescribed in the ITM Strategic Plan and the DII Master Plan. The ITM Strategic Plan establishes goals and objectives (ends), performance measurements and strategies (ways), and the required resources (means) to accomplish the policy vision goals.

Specifically, the ITM Strategic Plan[9]:

- Links ITM to joint warrior operational needs and mission support needs.

- Helps coordinate and integrate ITM activities across functional areas and organizations.

- Creates broad mechanisms to systematically manage DoD ITM resources and programs.

- Complies with the Information Technology Management Reform Act of 1996 (ITMRA).

- Serves as a model plan for ITM strategic plans at other levels and in other functions.

To accomplish these objectives, the ITM Strategic Plan outlines priority information and information technology initiatives, and facilitates the identification of common efforts and overlapping missions.

To accomplish Goal 1; "Become a mission partner", the planned objectives are to increase and promote IT interaction with mission, serve mission information users as customers, and facilitate process improvement. This requires joint interaction to assess missions, and apply interoperable and secure capabilities exploring IT concepts as end users.

To accomplish GOAL 2; "Provide services that satisfy customer information needs", the planned objectives are to build architecture and performance infrastructures, modernize and integrate defense information infrastructure, upgrade the technology base, and improve IT management tools. This can be extended into the architecture of the DII Master Plan to include products, services and performance measurements. Sharing secure data is key to interoperability and quality data.

To accomplish GOAL 3; "Reform IT management processes to increase efficiency and mission contribution", the planned objectives are to institutionalize ITMRA provisions, institute fundamental IT management reform efforts, and upgrade the DoD IT workforce. As resources decline, information and information technology must be managed as a strategic resource. All levels of the DoD must strive for reduced costs and streamlined processes. This can be accomplished through performance measurement and planning strategy.

To accomplish GOAL 4; "Ensure DoD's vital information resources are secure and protected", the planned objectives are to build an Information Assurance framework, build an Information Assurance architecture and support service, improve acquisition processes and regulations, and assess Information Assurance posture of DoD operational systems. Absolute security is not feasible, but a robust and resilient security system is vital to detecting intrusion, and restoring services and systems needs developed in the Defense Information Infrastructure.

The DoD IMT Strategic Plan, with the DII Master Plan as the support architecture, provides that each DoD Component maintain a DoD Component Strategic Plan, and that their plan "...will inherit the DoD goals and strategies and identify supporting initiatives[10]". Further, the DoD Component will use this guidance to prepare their plans and programs in support of their unique missions. The ITRMA requires an annual report be submitted with their budget showing actual results based on a strategic plan.

The DoD IMT Strategic Plan provides guidance for performance and assessment in achieving the strategic planning goals. The DoD Chief Information Officer will ensure that the performance measures are implemented for each strategy and goal. Collecting and coordinating with each affected Component will provide performance information and will be used to prepare the annual report and update the ITM Strategic Plan. The IMT Strategic Planning cycle is aligned with the Planning, Programming, and Budget System (PPBS).

Performance measurement can be accomplished through; self assessment using the Baldridge criteria (Presidential Quality Award criteria for government), through benchmarks using new processes or comparison to performance of others, or through surveys such as the DoD Comptroller Performance Assessment which determines how others perceive an organization, its services, and procedures.

The Assistant Secretary of Defense (ASDC3I) formed a Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) task force to address integration and interoperability. C4ISR provides an architectural and programmatic framework for integrating and rationalizing the infrastructure of functional areas ASD(C3I) is responsible for[11]. C4ISR task force recommendations include implementation of a common architecture, and strengthening the policy for compatibility, interoperability, integration and security. To achieve common architectures, military infrastructures need to explore leading edge concepts and advanced commercial technologies to achieve interoperability and security in systems, and to "break down the stovepipes" of current service systems.

The Military Services continue to develop information system strategies "complementary" to the C4I task force vision, but they still do not provide a unified picture of the information environment, they have a reduced ability to provide a link to the power projection support base, and they have limited connectivity to the US industrial base[12]. Stovepiping of systems is still occurring in all the services.

The Navy is moving toward implementing Information Technology 21, based on the Copernicus Architecture of information-pull rather than producer-push, for the operational and theater strategic commander. This system ties the afloat command, the fleet command, the Joint Task Force, the CINC command together in the Global Information Exchange System[13].

The Army's Enterprise Strategy provides for information needs as a Military Department, a force component, and a sustaining force for the CJTF. The Air Force Horizon Strategy provides C4I systems services in support of the Joint Staff C4I task force joint interoperability objectives.

The Marine Corps has a three-fold approach; a C4I common software suite, a common hardware suite to support software applications, and a common information transfer system and digital technical control[14].

A interim fix to achieve increased interoperability (in some cases) is Middleware, a commercial off the shelf (COTS) software that allows the user to see data on existing "stove-pipe" applications while information is stored, retrieved, and processed on a shared application known as the Migration System. This is a transition process, until more effective ways are standardized. The Military Communications Electronics Board (MCEB) is the resolution authority for the Military Services, Unified Combatant Commands, and Defense Agencies to help in the resolution of issues related to interoperability and standards[15].

The report of the Defense Science Task Force Board on Information Warfare - Defense recommends we establish a joint office for system, network and infrastructure design. This office will: "...develop and promulgate IW-D policies, architectures, and standards; design the information infrastructure for utility, resiliency, repairability, and security; develop and implement an IW-D configuration management process; and conduct independent verification of design and procurement specifications to ensure compliance with the design[16]."

To this point, we have established that we in the military have an immense reliance on information systems, at all levels, tactical, operational and strategic. And we are taking steps in the evolution of these infrastructures as required to support the National Military Strategy (NMS) statement; "...we will leverage emerging technologies to enhance the capabilities of our servicemen and women through development of new doctrine, organizations, material and training[17]."

The National Security Strategy (NSS) further expresses our dependency on the information infrastructure with the statement; "The national security posture of the United States is increasingly dependent on our information infrastructures. These infrastructures are highly interdependent and are increasingly vulnerable to tampering and exploitation... we must fully implement ... to ensure the future security of not only our national information infrastructures, but our nation as well[18]."

We have and continue to integrate the government (military) and civilian (commercial) aspects of information infrastructure, and have established our military dependency on commercial systems.

"Approximately 95 percent of all military communications are routed through commercial lines[19]". Further expansion of our military information infrastructure into the commercial sector is inevitable.

The Defense Information Infrastructure (DII) uses the National Information Infrastructure (NII) commercial overseas information infrastructure to meet the global information needs of the DoD. The NII has a federal initiative at work with industry, and state and local government, to develop a high-speed information processing and transfer network. It's evolution includes national telecommunications policy reform to encourage "growth of the information industry[20]".

Telecommunications reform recommendations made at the G7 countries meeting in Midrand, South Africa in May 1996 fully supports telecommunications liberalization; "As the information infrastructures and the GII evolve, markets and private investment will work to best ensure universal access to the networks and information resources people will need.[21]"

Commissioner Rachelle Chong of the United States Federal Communications Commission in her "thinking outside the box" article "Thoughts on The US Telecommunications Act of 1996" proposes that through this Act; "Congress has given the Americans the keys to enter the information age[22]", and fully supports this telecommunications liberalization with a three stage approach. Phase one of which is that government tear down existing barriers. Phase two is to tailor regulation to boost competition. And phase three is to let market forces take place of most regulatory solutions, provide that government should step back, and FCC oversight should be limited to light regulatory touch.

The primary means of information transmission is accomplished through the telecommunications infrastructure and one of the most common tools (protocols) used to do this is the Internet. A review in The Economist (July 1, 1995) refers to the Internet as the "accidental superhighway[23]".

The Secretary-General of the International Telecommunications Union Dr. Pekka Tarjanne in a keynote speech to a telecommunications union on Internet evolution refers to the Internet as the "global information infrastructure". He proposed several key issues[24] which parallel some of the concerns discussed so far (summarized);

* Will the Internet evolve to match expectations, ... what are the limitations, ...what about unstructured and unsorted information?

* There is no user protection for quality, reliability or desirability of information being accessed.

* The protocol is not optimized for multimedia traffic. ...It is cheap for end-users, ...not efficient.

He then proposes four scenarios [5] for future Internet development;

* Status Quo, incrementally improving in bandwidth availability and performance.

* Splintering into a series of interconnected and parallel, but application specific Internets.

* Worsening service quality, causing Internet collapse to a community of academics and enthusiasts.

* And finally, an alternative information infrastructure might emerge, offering better performance, which will replace the Internet.

Some of these scenarios for Internet development are not very likely, but whichever scenario eventually develops, one very difficult aspect of the development that will certainly require more attention is network security.

Network requirements are exploding for reliable, secure, efficient shared information repositories to support systems data and the World Wide Web[25].

There are a number of "wild card " scenarios that could seriously challenge U.S. interests both at home and abroad. Such scenarios range from unanticipated emergence of new technological threats, to the loss of U.S. access to critical facilities and lines of communication in key regions[26]. "One billion dollars and 20 capable hackers,...could shut down America[27]". How do you provide for the protection of critical information systems? The answer is in Information Assurance.

The ITM Strategic Plan defines Information Assurance as "the protection, integrity, and availability of critical information systems[28]". The issue of protection, integrity, and availability has been addressed in the fundamental information security requirements and techniques outlined in the Joint Staff Information Warfare Legal, Regulatory, Policy, and Organizational considerations for Information Assurance report[29]. The report highlighted our critical reliance on information infrastructure and provides several recommendations for information assurance. A general overview of these recommendations are as follows:

* Authentication - the verification of the identity of an individual or the source of information It can be thought of in terms of traditional passwords or personal identification numbers. It can also be achieved by other devices such as tokens, smart cards, or biometric devices attributable to an individual.

* Encryption - the transformation of data into a form unreadable by anyone without the appropriate decryption key. Encryption allows secure transmission over otherwise unsecure systems.

* Communications - the proliferation of high volume data exchange systems. Industry is driving the market and technological advances in increased communications. Several different protocols are offered which differ in implementation, but they all allow for extensive growth in bandwidth.

* Firewalls, Guards, and Multilevel devices - Firewalls filter network traffic from reaching protected computers and can effectively secure networks in many cases. Firewalls provide different levels of protection depending on the vendor, but provide one of the more effective protection mechanisms when properly installed. Guards are processors that limit the exchange of information between systems. They generally operate on strict formatting rules and provide effective means of segregating messages with differing classifications. Multilevel devices are trusted systems or equipment which process information with differing classifications or categories and permits simultaneous access by users with different security clearances, denying access to areas for those users who lack authorization (these systems are currently fielded within portions of the DoD).

* Wrappers - the Defense Advanced Research Projects Agency Information Science and Technology office commissioned a study to determine whether the nation's critical information infrastructure

could be hardened to improve survivability against a wide range of possible intentional or accidental threats. The study suggested a concept of wrappers to satisfy this requirement.

This concept allows the superimposition of a framework with a well specified structure to capture the critical elements of the underlying system, and then offers a form of leverage with which to introduce robustness into the system solution. The concept requires intercepting the Input/Output of existing components, applications, and data to provide additional capabilities for fault tolerance, security, intrusion detection, and system reconfiguration and management.

The Joint Staff recommendations point out several areas which may appear unique to the defense oriented information infrastructure, but they are not. The proprietary nature of private business and industry, the involvement of industry in development, and the provisions for security measures are at least equal in concern.

## Conclusion and recommendations for infrastructure development

The Information Age is in an evolutionary status, driven primarily by systems and technologies developed by the commercial sector. To achieve the common goals of the Global, National, and Defense Information Infrastructures the Department of Defense needs to work closely with private industry when researching existing and emerging information technologies in the process of developing or expanding information infrastructures.

The Joint Staff report on Information Warfare (July 1996) nicely summarizes many of the concerns we have discussed so far. "The evolution of the information Infrastructure is influenced by a wide variety of stakeholders with complex, diverse, and sometimes competing interests"... "The proliferation of new and emerging technologies complicates the information... equation..., commercial markets alone now influence the deployment of advanced information technologies and the DoD finds itself following the lead[30]". DoD may not have the lead, but we cannot and should not be far behind.

Department of Defense centralized policy and agency control as recommended by the Defense Science Task Force Board on Information

Warfare (Defense) is to establish a joint office for system, network and infrastructure design. This would provide a necessary link to private industry and help minimize services stovepiping development of infrastructures.

The US Telecommunications Act of 1996 will enhance the national efforts for the development of the Global and National Information Infrastructure and provide for telecommunications industry liberalization.

Critically important is the issue of network security measures. The Office of the Secretary of Defense in the Quadrennial Defense Review stated; "The capabilities to protect information systems must also extend beyond traditional military structures into the areas of civilian infrastructure that support national security requirements[31]."

The Joint Staff report best sums up most of the issues discussed in this paper with this statement; "The dependency of critical national economic and security functions on domestic infrastructures is one of significant challenges. ...The information infrastructure is and extremely complex interconnection of numerous government, public, and private networks. More research is needed regarding the functional dependencies on the infrastructure, the vulnerabilities of the infrastructure, a risk-management based approach to protection, or the means and methods to restore and reconstitute in the event of a successful attack[32]".

Word Count (excludes endnotes/bibliography) = 4,809

# ENDNOTES

[1] National Defense University Institute for National Strategic studies, Strategic Assessment 1996. (Washington D.C.), 1996.

[2] Daniel S. Paap, David S. Alberts, and Alissa Tuyahov, "Histrical Impacts of Information Technologies: An Overview", Information Age Anthology, Volume 1, Part 1, (National Defense University, Washington D.C.), 30.

[3] Ibid., 84.

[4] Global Information Infrastructure Commission, "The GIIC Mission Statement"; available from <http://www.gii.org/egi00180.html>; Internet; accessed 28 January 1998.

[5] Online Public Policy, "National Information Infrastructure"; available from <http://www2.itic.org/itic/niipol.htm>; Internet; accessed 16 December 1997.

[6] Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), Information Management Technology (ITM) Strategic Plan, Version 1.0 (Washington D.C.); available from <http://www.dtic.dla.mil/c3i/cio/references/itmstpln/itmstpln.html>; Internet; accessed 30 October 1997, 3.

[7] Ibid.

[8] Defense Information Systems Agency, Defense Information Infrastructure Master Plan, Version 6.0 (Washington D.C.); available from <http://www.disa.mil/diimp/diimp-1.html>; Internet; accessed 25 November 1997, Section 2.2.

[9] Office of the Assistant Secretary of Defense, 3.

[10] Ibid., 18.

[11] Defense Information Systems Agency, Section 2.5.2.5.

[12] Ibid., Section 3.1.

[13] Ibid., Section 2.5.2.6.

[14] Ibid., APPENDIX A.

[15] Ibid., Section 3.2.

[16] Office of the Under Secretary of Defense for Aquisition & Technology, "Report of the Defense Science Board Task Force on Information Warfare - Defense" (Washington D.C.); available from <http://www.jya.com/iwd.htm>; Internet; accessed 27 January 1998.

[17] Joint Chiefs of Staff, National Military Strategy, October 1997 (Washington D.C.); available from <http://www.dtic.mil/jcs/nmsl>; Internet; accessed 2 October 1997, 12.

[18] The White House, A National Security Strategy for a New Century (Washington D.C. 1997), 14.

[19] Bruce D. Berkowitz, "Warfare in the Information Age," Information Age Anthology, Volume 1, Part 3, (National Defense University, Washington D.C.), 524.

[20] Defense Information Systems Agency, Section 3.8.

[21] Information Technologies Industry Policy Document, "Global Information Infrastructure, Recommendations to the G7 Meeting in Mirand, South Africa", May 1996; available from <http://www2.itic.org/itic/iss_pol/ppdocs/giippr.htm>; Internet; accessed 25 February 1998.

[22] Rachelle Chong, "Thoughts on the US Telecommunications Act of 1996 and its Implications for Information Infrastructure Policies"; available from <http://www.ncb.gov.sg/nii/96scan4/chngbox.html>; Internet ; accessed 28 January 1998.

[23] National Computer Board, "The Internet and the Information Infrastructure: What's the Difference?"; available from <http://www.ncb.gov.sg/nii/96scan2/itu.html>; Internet; accessed 28 January 1998.

[24] Ibid.

[25] Office of the Assistant Secretary of Defense, 13.

[26] Office of the Secretary of Defense, Report of the Quadrennial Defense Review (Washington D.C.), 5.

[27] Walter Lagueur, "Postmodern Terrorism," *Foreign Affairs*, Vol.75, No. 5, September/October 1996, 35.

[28] Office of the Secretary of Defense, 50.

[29] The Joint Staff, Information Warfare, Legal. Regulatory, Policy, and Organizational Considerations for Assurance, 2nd Edition, (Washington D.C.) 1996.

[30] The Joint Staff, 4-1.

[31] Office of the Secretary of Defense, 50.

[32] The Joint Staff, 4-2.

## BIBLIOGRAPHY

National Defense University Institute for National Strategic studies, Strategic Assessment 1996. Washington D.C., 1996.

Papp, Daniel S., David S. Alberts, and Alissa Tuyahov, "Histrical Impacts of Information Technologies: An Overview", Information Age Anthology, Volume 1, Part 1, National Defense University, Washington D.C., June 1997.

Global Information Infrastructure Commission, "The GIIC Mission Statement". Available from <http://www.gii.org/egi00180.html>. Internet. Accessed 28 January 1998.

Online Public Policy, "National Information Infrastructure". Available from <http://www2.itic.org/itic/niipol.htm>. Internet. Accessed 16 December 1997.

Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), Information Management Technology (ITM) Strategic Plan, Version 1.0. Washington D.C. Available from <http://www.dtic.dla.mil/c3i/cio/references/itmstpln/itmstpln.html>. Internet. Accessed 30 October 1997.

Defense Information Systems Agency, Defense Information Infrastructure Master Plan, Version 6.0. Washington D.C. Available from <http://www.disa.mil/diimp/diimp-1.html>. Internet. Accessed 25 November 1997.

Office of the Under Secretary of Defense for Aquisition & Technology, "Report of the Defense Science Board Task Force on Information Warfare - Defense". Washington D.C. Available from <http://www.jya.com/iwd.htm>. Internet. Accessed 27 January 1998.

Joint Chiefs of Staff, National Military Strategy, October 1997. Washington D.C. Available from <http://www.dtic.mil/jcs/nmsl>. Internet. Accessed 2 October 1997.

The White House, A National Security Strategy for a New Century Washington D.C., May 1997.

Berkowitz, Bruce D., "Warfare in the Information Age," Information Age Anthology, Volume 1, Part 3. National Defense University, Washington D.C. June 1997.

Information Technologies Industry Policy Document, "Global Information Infrastructure, Recommendations to the G7 Meeting in Mirand, South Africa", May 1996. Available from <http://www2.itic.org/itic/iss_pol/ppdocs/giippr.htm>. Internet. Accessed 25 February 1998.

Chong, Rachelle, "Thoughts on the US Telecommunications Act of 1996 and its Implications for Information Infrastructure Policies". Available from <http://www.ncb.gov.sg/nii/96scan4/chngbox.html>. Internet. Accessed 28 January 1998.

National Computer Board, "The Internet and the Information Infrastructure: What's the Difference?". Available from <http://www.ncb.gov.sg/nii/96scan2/itu.html>. Internet. Accessed 28 January 1998.

Office of the Secretary of Defense, Report of the Quadrennial Defense Review. "Information assurance" - the protection, integrity, and availability of critical information systems and networks." Washington D.C. 1997:

Walter Lagueur, "Postmodern Terrorism," *Foreign Affairs*, Vol.75, No. 5, September/October 1996.

The Joint Staff, Information Warfare, Legal. Regulatory, Policy, and Organizational Considerations for Assurance, 2nd Edition, Washington D.C., 4 July 1996.